TI - Method for increasing the protection against theft of portable devices, such as mobile phones by ensuring that if a linked device, such as a SIM card, is removed before an activation code is entered, the device is blocked

AB - FR2818474 NOVELTY - Method comprises loading in a portable device (1) of security software including an activation code (Ca) unique to a user and necessary to break a dependence link between a detachable device (6, 6') and the portable device, entry of the code by a user and if the code is correct breaking of the dependence link. If the detachable device is removed before a code has been entered, the device is automatically blocked.

- DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also made for
- (1) an assembly of a portable device and a detachable element associated with it
- (2) installation with a central unit and a collection of associated portable devices
- USE - Method for increasing the protection against theft of portable devices, such as mobile phones, PDAs and any other mobile device.
- ADVANTAGE - If a dependence link is broken between a portable device and an associated detachable element, e.g. a mobile phone and a SIM card, before an authentication code has been entered, then the device or phone is blocked. The device security is significantly increased reducing theft temptation.
- DESCRIPTION OF DRAWING(S) - Figure shows a mobile phone according to the invention.
- mobile phone 1
- activation code Ca
- SIM card6, 6'
- external control center. 2
- (Dwg.2/2)

PR - FR20000016486 20001218

PN - FR2818474 A1 20020621 DW200258 H04L9/32 024pp
- WO0251106 A1 20020627 DW200258 H04M1/66 Frn 000pp
- AU200219308 A 20020701 DW200264 H04M1/66 000pp

PA - (TOFF-I) TOFFOLET R

IC - G06F17/30 ;G07F7/10 ;H04L9/32 ;H04M1/66 ;H04Q7/32

IN - TOFFOLET R

OPD - 2000-12-18

DN - AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN I JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG US UZ VN YU ZA ZM ZW

DS - BE CY EA FR GR IE IT MC NL OA SZ

AN - 2002-540521 [58]

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 818 474**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **00 16486**

(51) Int Cl[7] : **H 04 L 9/32**, G 07 F 7/10, H 04 M 1/66, G 06 F 17/30, H 04 Q 7/32

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 18.12.00.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 21.06.02 Bulletin 02/25.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *TOFFOLET RICHARD* — FR.

(72) **Inventeur(s) :** TOFFOLET RICHARD.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :** CABINET SAUVAGE.

(54) PROCEDE DE LUTTE CONTRE LE VOL DE DISPOSITIFS "NOMADES", DISPOSITIF ET INSTALLATION CORRESPONDANTE.

(57) Le procédé est applicable aux dispositifs (1) dont le fonctionnement peut être asservi à un logiciel et qui ont un lien de dépendance avec au moins un composant amovible, dit " composant en place (6, 6') ".

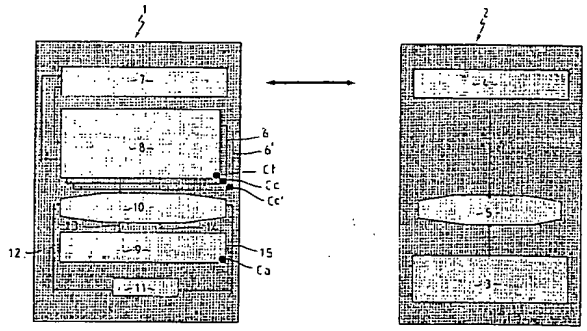
Il comprend:

a) le chargement, dans le dispositif (1), d'un logiciel de protection où est inscrit un code d'activation (C_a) personnel à l'utilisateur et nécessaire pour pouvoir rompre ledit lien de dépendance,

b) la fourniture de ce code (C_a) à l'utilisateur,

et, si ledit code (C_a) n'a pas été entré dans le dispositif (1) préalablement à la rupture dudit lien de dépendance:

c) le blocage du fonctionnement du dispositif (1), sous la commande du logiciel de protection.



FR 2 818 474 - A1

La présente invention concerne le domaine de la lutte contre le vol ou l'utilisation frauduleuse de dispositifs dont le fonctionnement est susceptible d'être asservi à un logiciel, les dispositifs correspondants ainsi qu'une installation permettant la mise en oeuvre de ce procédé.

Il peut s'agir, en particulier, de terminaux de communication, c'est-à-dire, dans le sens donné ici à cette expression, de toute structure permettant une communication (émission / réception) avec un émetteur-récepteur externe, qu'il s'agisse de la ou d'une fonction essentielle de ladite structure, comme dans le cas de téléphones mobiles, d'ordinateurs portables, etc., ou d'une fonction rendue possible par les moyens susceptibles d'y être inclus, comme dans le cas d'un véhicule automobile, d'un bateau, d'un avion, etc.. Il peut encore s'agir d'appareils n'assurant pas normalement de fonction de communication tels que caméscopes, appareils photographiques, etc.

Actuellement, le développement des nouvelles technologies va vers le "tout portable", d'où une multiplication des appareils ou dispositifs de communication dits "nomades", c'est-à-dire portables ou intégrables dans divers environnements ou, plus simplement, dont le fonctionnement n'est pas attaché à un lieu précis. Ce développement d'une nouvelle génération d'appareils portables, donc relativement petits et légers, s'est accompagné d'une augmentation des vols et/ou des utilisations frauduleuses suite à leur perte.

Un intérêt croissant a donc été porté au développement de systèmes permettant d'empêcher l'utilisation des appareils volés ou égarés, dissuadant ainsi tout voleur potentiel de passer à l'acte et encourageant la remise aux objets trouvés des appareils perdus.

En matière de téléphones mobiles, une première approche a consisté à mettre à profit le fait que certains appareils sont "dédiés", c'est-à-dire qu'ils comportent une ligne de programmation supplémentaire telle qu'ils ne

peuvent fonctionner avec une autre carte SIM (d'après la nomenclature anglaise "Subscriber Identity Module") que celle qui a été fournie avec l'abonnement souscrit auprès d'un opérateur. Il est possible, en cas de vol ou de perte de l'appareil, d'en informer l'opérateur pour qu'il bloque l'abonnement.

Cependant, l'interruption de l'abonnement n'est pas automatique mais nécessite l'intervention de l'utilisateur auprès de l'opérateur.

De plus, ce procédé ne convient pas aux appareils dans lesquels la carte SIM peut être remplacée par une autre carte SIM. Il faudrait donc pouvoir bloquer, non pas l'abonnement, mais l'appareil lui-même.

Un procédé connu utilise, pour les téléphones mobiles, un système de codes, dits codes PIN (d'après la nomenclature anglaise "Personal Identification Number") que l'utilisateur choisit lui-même et qu'il entre dans la mémoire du téléphone. L'appareil a besoin du ou des code(s) PIN pour pouvoir lire la carte SIM et permettre l'utilisation de l'appareil. Par suite, à chaque mise sous tension, l'utilisateur doit entrer le ou les code(s) PIN, ce qui limite les risques d'utilisation frauduleuse de l'appareil, mais est extrêmement fastidieux. De plus, si le téléphone est volé alors qu'il se trouve sous tension, il suffit au voleur de ne pas le mettre hors tension pour pouvoir l'utiliser. Ce procédé présente, en outre, l'inconvénient de nécessiter l'entrée d'un ou plusieurs codes, dont les fonctions sont souvent mal comprises par les utilisateurs, ce qui débouche sur des erreurs de manipulation entraînant le blocage intempestif de l'appareil. De plus, les codes PIN utilisés sont facilement décryptables, ce qui en réduit l'utilité.

Un tel procédé de blocage utilisant différents codes PIN et le code IMSI (d'après la nomenclature anglaise "International Mobile Subscriber Identity") stocké dans la carte SIM est décrit dans EP 0 607 767.

L'invention a pour but de remédier aux inconvénients de la technique antérieure et pour ce faire, selon un premier aspect, elle propose un procédé pour la lutte contre le vol et/ou l'utilisation frauduleuse d'un dispositif dont le fonctionnement est susceptible d'être asservi à un logiciel et qui a un lien de dépendance avec au moins un composant amovible, dit "composant en place",

caractérisé en ce qu'il comprend les étapes suivantes :

a) le chargement, dans ledit dispositif, d'un logiciel de protection dans lequel est inscrit un code d'activation personnel à l'utilisateur et qui lui est nécessaire pour pouvoir rompre ledit lien de dépendance,

b) la fourniture à l'utilisateur autorisé dudit code d'activation,

et, si ledit code d'activation n'a pas été entré dans le dispositif préalablement à la rupture dudit lien de dépendance :

c) le blocage du fonctionnement du dispositif, sous la commande dudit logiciel de protection.

Dans la présente description et dans les revendications, il faut entendre par :

- "composant amovible", tout élément aussi bien matériel (tel qu'une carte à puce, un périphérique informatique, etc.) qu'immatériel (tel qu'un logiciel par exemple) avec lequel le dispositif a un lien de dépendance ;

- par "lien de dépendance", le fait que le composant amovible est nécessaire au fonctionnement du dispositif (telle qu'une carte SIM pour un téléphone mobile ou un film pour un appareil photographique) ou, plus généralement, le fait que le composant amovible est physiquement réuni audit dispositif, qu'il soit ou non nécessaire à son fonctionnement (telle qu'une imprimante à une unité centrale d'ordinateur), étant entendu qu'un même dispositif peut avoir un lien de dépendance avec plusieurs composants amovibles ;

- par "clé", tout code transmissible à distance et propre soit audit composant, tel que le code IMSI d'une carte SIM, soit au dispositif, tel qu'un code IMEI (d'après la nomenclature anglaise "International Mobil Equipment Identity").

On aura compris que l'invention met à profit le fait que la première démarche commise sur un dispositif dont le voleur ou l'utilisateur frauduleux peut être identifié ou localisé à partir de la clé de composant du composant en place, comme par exemple le code IMSI de la carte SIM d'un téléphone mobile, est l'extraction du composant en place en vue de sa substitution par un composant équivalent. De même, s'agissant du vol, par exemple, d'un ordinateur, la première démarche du voleur sera de le débrancher de ses périphériques. En contrôlant la licéité de cette extraction ou de ce débranchement, le procédé selon l'invention rend le vol sans intérêt et l'utilisation frauduleuse impossible, ce de façon très simple puisqu'il suffit à l'utilisateur de se faire enregistrer par le gestionnaire du service de protection et de charger dans son dispositif le logiciel de protection pour avoir la garantie que le composant en place avec lequel son dispositif a un lien de dépendance ne pourra pas être extrait ou débranché par qui ne connaît pas le code d'activation, sans qu'il en résulte le blocage dudit dispositif. Ce code d'activation n'est entré, dans le dispositif, par l'utilisateur autorisé que s'il désire remplacer le composant en place par un composant équivalent ou débrancher momentanément le composant en place pour une raison ou pour une autre, ce qu'il fait peu fréquemment ; la protection du dispositif n'implique donc aucune manipulation répétée et fastidieuse.

Selon une forme d'exécution préférée de l'invention, le procédé comporte, en outre, une étape consistant en :

d) le déclenchement, sous l'effet de l'entrée du code d'activation dans le dispositif, d'une temporisation offrant le temps nécessaire à la rupture et au rétablissement du lien de dépendance, et le cas échéant

e) le blocage du dispositif, si le lien de dépendance n'a pas été rétabli avant la fin dudit temps de temporisation.

Par "temporisation", il faut comprendre toute action visant à fixer une durée prédéterminée.

Par "rétablissement du lien de dépendance", il faut comprendre la substitution d'un composant équivalent au composant en place ou le rebranchement du composant en place débranché momentanément.

L'étape e) est prévue pour éviter que l'utilisateur autorisé puisse laisser la protection déverrouillée sans rétablir le lien de dépendance, ce qui permettrait, en cas de vol du dispositif dans cet état, l'utilisation dudit dispositif par un tiers.

Dans une forme d'exécution préférée, le procédé selon l'invention comporte, en outre, une étape consistant en :

f) le blocage du dispositif en cas d'entrées successives d'un nombre prédéterminé de codes d'activation erronés.

Le blocage du terminal pouvant résulter d'une erreur de l'utilisateur autorisé, le procédé selon l'invention prévoit avantageusement la possibilité d'une étape consistant en :

g) le déblocage dudit dispositif par le fournisseur du code d'activation.

Dans un mode d'exécution préféré appliqué au cas où le dispositif est un terminal de communication, ledit terminal et ledit composant en place ayant, chacun, des clés qui leur sont propres, dites respectivement "clé de terminal" et "clé de composant", le procédé comporte, en outre, les étapes consistant en :

h) l'enregistrement dans un équipement externe, comportant une base de données et un émetteur récepteur, d'au moins une donnée identifiant l'utilisateur autorisé dudit terminal ;

i) la communication par le terminal audit émetteur-récepteur de l'équipement externe de la clé de

terminal et de la clé de composant dudit composant en place lors de la première mise en oeuvre du procédé ;

j) l'enregistrement, dans ladite base de données, de la clé de terminal et de la clé de composant dudit composant en place, et,

en cas de substitution du composant en place par un composant équivalent dans les conditions prévues par le logiciel de protection,

k) la communication par le terminal audit émetteur-récepteur de l'équipement externe de la clé de terminal et de la clé de composant dudit composant équivalent, et

l) l'enregistrement dans la base de données de l'équipement externe de la clé de composant dudit composant équivalent, ce, à des fins de traçage.

Concomitamment au blocage du terminal et quelle qu'en soit la cause, en étape m), un message d'alerte peut être envoyé, depuis le terminal vers l'émetteur-récepteur de l'équipement externe, ou inversement, ou réciproquement, et éventuellement affiché.

La plupart du temps, il est stocké, dans le terminal que l'on souhaite protéger, des données dont la perte peut être extrêmement gênante (cas, par exemple, d'un répertoire téléphonique) ou ayant un caractère confidentiel.

Dans une forme d'exécution particulière du procédé selon l'invention, celui-ci comprend, en cas de blocage du terminal par suite de la mise en oeuvre de l'étape c), e) ou f) ci-dessus, une étape supplémentaire consistant en :

n) le transfert de tout ou partie des données stockées dans ledit terminal vers la base de données dudit équipement externe et/ou

o) la destruction de tout ou partie des données stockées dans le terminal.

Ainsi, dans le cas de l'étape n), l'utilisateur autorisé pourra récupérer tout ou partie de ses données depuis la base de données appartenant à l'équipement externe, base qui les stockera et les restituera à

l'utilisateur autorisé, par téléchargement ou par l'intermédiaire de tout support approprié.

L'étape o) pourra consister à détruire soit uniquement les données qui ont été transférées au cours de l'étape n) décrite plus haut, soit uniquement des données qui ont été sélectionnées préalablement, par exemple lors de leur entrée dans le terminal, soit encore toutes les données stockées dans ledit terminal de communication. Un tel procédé est particulièrement utile dans le cas des ordinateurs portables pour permettre la destruction de tous les fichiers personnels ou que l'utilisateur autorisé désire garder secrets.

Le logiciel nécessaire à la mise en oeuvre du procédé selon l'invention et/ou son éventuel déblocage sera, de préférence, téléchargeable sur le terminal depuis l'équipement externe. Si le terminal n'est capable ni de recevoir un tel téléchargement, ni d'être chargé à partir d'un support quelconque (disquette, CD-ROM, etc.), une nécessaire adaptation devra être effectuée par le constructeur.

Selon un second aspect de la présente invention, celle-ci concerne un ensemble formé, d'une part, par un dispositif dont le fonctionnement est susceptible d'être asservi à un logiciel et, d'autre part, par au moins un composant amovible, dit "composant en place", avec lequel ledit dispositif a un lien de dépendance,

ledit dispositif étant chargé d'un logiciel de protection où est inscrit un code d'activation personnel à l'utilisateur autorisé du dispositif et qui est adapté :

α) à permettre à l'utilisateur autorisé de rompre momentanément le lien de dépendance entre son terminal et ledit composant amovible, et

β) à bloquer le terminal, s'il advient que le code d'activation n'a pas été entré préalablement à la rupture du lien de dépendance.

Avantageusement, le dispositif peut comprendre en outre :

γ) des moyens de déclenchement, sous l'effet de l'entrée de son code d'activation, d'une temporisation offrant le temps nécessaire à la rupture et au rétablissement du lien de dépendance, et

δ) des moyens de blocage agissant sur le dispositif si ledit lien de dépendance n'a pas été rétabli avant la fin du temps de temporisation.

Il peut comprendre en outre :

ε) des moyens de blocage agissant sur le dispositif en cas d'entrées successives d'un nombre prédéterminé de codes d'activation erronés.

Pour la mise en oeuvre des différentes étapes décrites plus haut à propos du procédé appliqué au cas d'une pluralité de dispositifs constitués chacun d'un terminal de communication ayant un lien de dépendance avec au moins un composant amovible, dit "composant en place", chaque terminal et chaque composant amovible comportant des clés qui leur sont propres, dites, respectivement, "clé de terminal" et "clé de composant", l'invention apporte une installation constituée d'une pluralité de tels terminaux et d'un équipement externe comprenant un émetteur-récepteur et une base de données adaptée à enregistrer, pour chaque terminal, au moins une donnée identifiant l'utilisateur autorisé, et les informations de clé de terminal et de clé de composant qui lui sont communiquées par ledit terminal.

Bien entendu, si un terminal donné a un lien de dépendance avec plusieurs composants en place et que plusieurs de ces composants en place ont été remplacés par des composants équivalents dans les conditions autorisées par le logiciel de protection, le terminal peut communiquer à l'équipement externe la clé de composant de chacun des composants équivalents de substitution.

L'installation peut, en outre, comporter :

ζ) des moyens d'envoi, en cas de blocage d'un terminal, d'un message d'alerte du terminal concerné vers l'émetteur-récepteur de l'équipement externe, ou inversement, ou réciproquement, et éventuellement des

moyens d'affichage d'un tel message, lesquels moyens d'envoi/affichage sont activés concomitamment avec lesdits moyens de blocage.

L'installation comprend, de préférence, également :

η) des moyens de déblocage d'un terminal bloqué, moyens qui sont susceptibles d'être mis en oeuvre depuis l'équipement externe.

Appliquée à la protection de terminaux dans lesquels sont stockées des données, l'installation comprend avantageusement :

θ) des moyens de transfert de tout ou partie des données stockées dans le terminal concerné vers la base de données dudit émetteur-récepteur externe en cas de blocage d'un terminal et/ou

ι) des moyens de destruction de tout ou partie des données stockées dans ledit terminal en cas de blocage de celui-ci.

L'invention sera mieux comprise, et ses avantages ressortiront mieux, à la lumière de la description détaillée suivante faite en référence aux dessins annexés dans lesquels :

la figure 1 représente un diagramme en flux illustrant un mode de mise en oeuvre du procédé selon l'invention, appliqué à la protection d'un téléphone mobile et

la figure 2 est une représentation schématique d'une forme d'exécution de l'installation selon l'invention, d'application plus généralisée.

Si l'on se reporte à la figure 1, on voit les différentes étapes d'un mode de mise en oeuvre du procédé selon l'invention, mise en oeuvre qui nécessite le recours à un fournisseur de services, gestionnaire de ce qui a été appelé plus haut l'équipement externe.

La première étape, pour un utilisateur qui désire avoir recours aux services en question, consiste à faire enregistrer dans la base de données de l'équipement externe au moins une donnée permettant de l'identifier, donnée qui

peut consister, par exemple, en son nom, son adresse, son numéro de téléphone, etc.

Cet enregistrement effectué, l'utilisateur devient pour l'équipement externe un "utilisateur autorisé" et il lui est fourni, par le gestionnaire du système de protection, un code d'activation non modifiable du programme de déverrouillage/temporisation/verrouillage de son téléphone tel que géré par un logiciel de protection, lequel est téléchargé dans le téléphone depuis l'émetteur-récepteur de l'équipement externe. Le code peut être fourni à l'utilisateur autorisé par courrier ou tout autre moyen confidentiel. Le code d'activation est également inscrit par le gestionnaire du système de protection dans le logiciel téléchargé sans être accessible, depuis ce logiciel, à tout utilisateur du téléphone.

Au cours de la phase suivante, le téléphone mobile communique à l'équipement externe

- son code IMEI, et
- le code IMSI de la carte SIM qui l'équipe.

La protection contre le vol selon l'invention ne modifie en rien l'utilisation normale du téléphone par l'utilisateur autorisé.

Elle n'intervient qu'en cas de changement de la carte SIM.

Si l'utilisateur autorisé du téléphone souhaite remplacer la carte SIM en place (séquence 1), par exemple s'il prête son téléphone mobile à un tiers possédant sa propre carte SIM et désirant se servir du téléphone sur son propre abonnement, l'utilisateur autorisé doit entrer au préalable le code d'activation qui lui a été communiqué par le gestionnaire du service de protection.

Le code entré est comparé à celui qui a été inscrit, par le gestionnaire du service de protection, dans le logiciel téléchargé et, s'il est correct (séquence 1.A), cela a pour effet de déclencher une temporisation au cours de laquelle il peut être procédé à un échange de carte SIM.

Si l'échange a bien été effectué avant le terme de la période de temporisation, il s'effectue (séquence 1.A.1) un verrouillage automatique du téléphone avec communication, par le téléphone à l'émetteur-récepteur de l'équipement externe, du code IMEI du téléphone, pour identification de l'utilisateur autorisé, ainsi que du code IMSI de la carte SIM de substitution, code qui est mémorisé par la base de données de l'équipement externe et qui, par la suite, sera considéré comme étant la clé du composant en place, reconnu comme composant autorisé. Cette sauvegarde dans la base de données de l'équipement externe permet un traçage précis ainsi que des actions diverses de limitation de la fraude liée à l'usage du téléphone et de son ou ses composants amovibles.

Le téléphone fonctionne alors normalement, sans qu'il soit nécessaire d'effectuer une quelconque autre opération.

Si l'échange de carte SIM n'a pas été effectué avant le terme de la période de temporisation, le fonctionnement du téléphone est immédiatement bloqué (séquence 1.A.2).

Si l'utilisateur autorisé opère l'échange de façon trop lente et qu'il s'ensuive le blocage de son téléphone, il doit prendre contact avec le gestionnaire du service de protection pour en obtenir le déblocage.

Si le code d'activation entré au clavier dans le téléphone est incorrect (séquence 1.B), un message d'erreur s'affiche. Une répétition de trois erreurs successives entraîne le blocage du téléphone. Là encore, si les erreurs sont le fait de l'utilisateur autorisé, il peut obtenir le déblocage de son téléphone en prenant contact avec le gestionnaire du service de protection.

S'il y a extraction de la carte SIM en place sans entrée préalable du code d'activation (séquence 2), ce qui se produira le plus souvent en cas de vol du téléphone, il s'ensuivra le blocage automatique et immédiat du téléphone. Si cette extraction est le fait d'un utilisateur autorisé mais distrait, le déblocage pourra être obtenu comme indiqué plus haut.

En ce qui concerne le blocage, il s'effectue au moyen du logiciel chargé dans le téléphone, sans intervention de l'équipement externe, logiciel qui réagit à partir du moment où il y a tentative de substitution du composant en place par un composant équivalent sans entrée préalable du code d'activation, trois erreurs successives à l'entrée du code d'activation, ou dépassement du temps de temporisation après entrée du code d'activation correct. Un tel blocage peut être effectué par tout moyen connu de l'homme de l'art, par exemple la désactivation d'un organe du téléphone comme le blocage du fonctionnement des touches du clavier.

En ce qui concerne le déblocage, il s'effectue, comme on l'a vu plus haut, depuis l'équipement externe, en utilisant là encore tout moyen connu de l'homme de l'art, comme un téléchargement d'instructions de déblocage.

De préférence et quelle que soit la cause du blocage du téléphone, un message d'alerte sera envoyé, et éventuellement affiché, depuis le téléphone vers l'émetteur-récepteur externe, ou inversement, ou réciproquement. Ainsi, en cas de tentative de substitution non autorisée de la carte SIM ou en cas de dépassement du temps disponible pour une substitution autorisée, il pourra apparaître sur l'écran du téléphone un message "fonctionnement bloqué", ce qui, en cas de vol, signalera au voleur l'inutilité de son acte et, en cas de dépassement du temps de temporisation, informera l'utilisateur autorisé de la nécessité de prendre contact avec le gestionnaire du système de protection. Dans les mêmes circonstances, un message pourra être reçu ou affiché par l'émetteur-récepteur externe ce qui, en cas de vol du téléphone, pourra permettre au gestionnaire du service de protection d'aviser l'utilisateur autorisé que le fonctionnement de son dispositif perdu ou volé a été bloqué.

Dans une forme d'exécution préférée de l'invention, quelle que soit la raison du blocage du téléphone, les

données qui y sont contenues, par exemple le répertoire téléphonique, seront en tout ou partie transférées vers, et stockées dans, la base de données de l'équipement externe qui les restituera à l'utilisateur autorisé de toute manière convenable, de préférence par téléchargement depuis l'équipement externe, soit vers le téléphone dudit utilisateur autorisé s'il se trouve toujours en sa possession dans le cas d'un blocage de son fait, soit vers un nouveau téléphone de remplacement dans le cas d'un vol. Les données transférées vers la base de données de l'équipement externe et stockées à titre temporaire dans celle-ci pourront simultanément être détruites dans la mémoire du téléphone, empêchant ainsi toute personne autre que l'utilisateur autorisé d'y avoir accès.

Dans le cas où l'utilisateur autorisé souhaite ne plus utiliser le service de protection selon l'invention, il lui suffit (séquence 3) de résilier le contrat conclu avec le gestionnaire dudit service, l'équipement externe téléchargeant un programme de neutralisation du logiciel de protection précédemment téléchargé dans le téléphone, avec pour conséquence que le remplacement de la carte SIM en place par une autre redevient possible sans code d'activation.

Bien que l'on se soit référé ci-dessus, par commodité, à la protection d'un téléphone mobile, il est bien entendu que le procédé est applicable à tout terminal de communication, dans la définition qui est donnée plus haut, ou même, dans sa forme d'exécution la plus simple, à tout dispositif dont le fonctionnement est susceptible d'être asservi à un logiciel.

Si l'on se reporte maintenant à la figure 2, celle-ci représente un exemple d'installation conforme à la présente invention, d'application plus généralisée.

Plus particulièrement, l'installation est composée d'une série de terminaux de communication dont un seul 1 est représenté et d'un équipement externe 2 comportant une base de données 3 capable d'enregistrer, notamment, au

moins une donnée identifiant l'utilisateur autorisé et un code d'activation C_a pour chacun des terminaux, un émetteur-récepteur 4 qui est en communication avec lesdits terminaux et réciproquement, et un dispositif de traitement de l'information 5 mettant en relation ledit émetteur-récepteur 4 et ladite base de données 3. La communication peut être d'ordre électronique, magnétique, etc.

Chaque terminal de communication 1, auquel est associée une clé de terminal C_t, a un lien de dépendance avec au moins un composant amovible, dit composant en place 6, 6' auquel est associée une clé de composant C_c, C_c'. Le terminal 1 comprend un dispositif de communication 7 capable de communiquer avec l'émetteur-récepteur 4 de l'équipement externe 2, un espace de stockage 8 d'informations internes au terminal (clé de terminal C_t) ainsi que des informations internes à chaque composant en place (clés de composant C_c, C_c'), un espace de stockage 9 d'informations externes à l'appareil (logiciel de protection et code d'activation C_a) et une unité de traitement de l'information 10 mettant en relation les deux de espaces de stockage 8 et 9.

Le dispositif de communication 7 de chaque terminal est capable de communiquer à l'émetteur-récepteur 4 de l'équipement externe sa clé de terminal C_t et la ou les clés de composant C_c, C_c' de ses composants en place pour enregistrement dans la base de données 3. En outre, après une modification autorisée d'un des composants en place 6, 6' par un composant équivalent, ladite base de données 3 enregistre la clé de composant dudit composant équivalent.

Le terminal 1 comporte, en outre, un clavier 11 au moyen duquel le code d'activation C_a peut être entré dans le terminal et transmis selon 12 à l'unité de traitement de l'information 10 qui l'envoie selon 13 à l'espace de stockage 9 pour comparaison, par le logiciel de protection, avec le code d'activation qui y est inscrit. Selon 14 est retourné à l'unité de traitement 10 le résultat de la

comparaison. Si le code d'activation entré est correct, l'utilisateur peut extraire ou débrancher un composant en place 6 et remplacer ce composant ou le rebrancher dans le délai autorisé par le logiciel. Dans le cas contraire, le logiciel de protection envoie, selon 14, des instructions de blocage, par exemple de blocage du clavier 11 selon la ligne 15.

De telles instructions de blocage sont également envoyées, s'il advient que le composant en place 6 ou 6' est extrait sans entrer le code d'activation C_a.

Pour le reste, le fonctionnement se fait comme il a été décrit plus haut à propos de la figure 1, le cas échéant, mutatis mutandis.

Comme il ressort de la description qui précède, l'invention permet aussi bien d'empêcher l'utilisation d'un dispositif volé ou perdu, que de retrouver le propriétaire d'un dispositif trouvé. En outre, la protection s'exerçant en permanence, sans intervention de l'utilisateur, cela constitue un facteur favorable vis-à-vis des compagnies d'assurances.

REVENDICATIONS

1. Procédé pour la lutte contre le vol et/ou l'utilisation frauduleuse d'un dispositif (1) dont le fonctionnement est susceptible d'être asservi à un logiciel et qui a un lien de dépendance avec au moins un composant amovible, dit "composant en place (6,6')",

caractérisé en ce qu'il comprend les étapes suivantes :

a) le chargement, dans ledit dispositif (1), d'un logiciel de protection dans lequel est inscrit un code d'activation (C_a) personnel à l'utilisateur et qui lui est nécessaire pour pouvoir rompre ledit lien de dépendance,

b) la fourniture à l'utilisateur autorisé dudit code d'activation (C_a),

et, si ledit code d'activation (C_a) n'a pas été entré dans le dispositif (1) préalablement à la rupture dudit lien de dépendance :

c) le blocage du fonctionnement du dispositif (1), sous la commande dudit logiciel de protection.

2. Procédé selon la revendication 1, caractérisé en ce qu'il comporte, en outre, une étape consistant en :

d) le déclenchement, sous l'effet de l'entrée du code d'activation (C_a) dans le dispositif (1), d'une temporisation offrant le temps nécessaire à la rupture et au rétablissement du lien de dépendance, et le cas échéant

e) le blocage du dispositif (1), si le lien de dépendance n'a pas été rétabli avant la fin dudit temps de temporisation.

3. Procédé selon la revendication 1 ou 2, caractérisé en ce qu'il comporte, en outre, une étape consistant en :

f) le blocage du dispositif (1) en cas d'entrées successives d'un nombre prédéterminé de codes d'activation erronés.

4. Procédé selon l'une quelconque des revendications précédentes appliqué au cas où le dispositif (1) est un terminal de communication, ledit terminal (1) et ledit

composant en place (6,6') ayant, chacun, des clés qui leur sont propres, dites respectivement "clé de terminal (C_t)" et "clé de composant (C_c, C_c')", caractérisé en ce que le procédé comporte, en outre, les étapes consistant en :

h) l'enregistrement dans un équipement externe (2), comportant une base de données (3) et un émetteur-récepteur (4), d'au moins une donnée identifiant l'utilisateur autorisé dudit terminal (1) ;

i) la communication par le terminal (1) audit émetteur-récepteur (4) de l'équipement externe (2) de la clé de terminal (C_t) et de la clé de composant (C_c, C_c') dudit composant en place (6,6') lors de la première mise en oeuvre du procédé ;

j) l'enregistrement, dans ladite base de données (3), de la clé de terminal (C_t) et de la clé de composant (C_c, C_c') dudit composant en place (6,6'), et,

en cas de substitution du composant en place (6,6') par un composant équivalent dans les conditions prévues par le logiciel de protection,

k) la communication par le terminal (1) audit émetteur-récepteur (4) de l'équipement externe (2) de la clé de terminal (C_t) et de la clé de composant dudit composant équivalent, et

l) l'enregistrement dans la base de données (3) de l'équipement externe (2) de la clé de composant dudit composant équivalent.

5. Procédé selon la revendication 4, caractérisé en ce qu'il comporte une étape supplémentaire consistant en :

m) l'envoi d'un message d'alerte depuis le terminal (1) vers l'émetteur-récepteur (4) de l'équipement externe (2), ou inversement, ou réciproquement, et éventuellement son affichage.

6. Procédé selon la revendication 4 ou 5, caractérisé en ce qu'il comprend, en cas de blocage du terminal (1) par suite de la mise en oeuvre de l'étape c), e) ou f) ci-dessus, une étape supplémentaire consistant en :

n) le transfert de tout ou partie des données

stockées dans ledit terminal (1) vers la base de données (3) dudit équipement externe (2) et/ou

o) la destruction de tout ou partie des données stockées dans le terminal (1).

7. Procédé selon l'une quelconque des revendications 4 à 6, caractérisé en ce qu'il consiste à débloquer un terminal (1) bloqué par téléchargement sur ledit terminal, depuis l'équipement externe (2), d'instructions de déblocage.

8. Ensemble formé, d'une part, par un dispositif (1) dont le fonctionnement est susceptible d'être asservi à un logiciel et, d'autre part, par au moins un composant amovible, dit "composant en place (6,6')" avec lequel ledit dispositif (1) a un lien de dépendance,

caractérisé en ce que ledit dispositif (1) est chargé d'un logiciel de protection où est inscrit un code d'activation (C_a) personnel à l'utilisateur autorisé du dispositif (1) et qui est adapté :

α) à permettre à l'utilisateur autorisé de rompre momentanément le lien de dépendance entre son terminal (1) et ledit composant en place (6,6'), et

β) à bloquer le terminal (1), s'il advient que le code d'activation (C_a) n'a pas été entré préalablement à la rupture du lien de dépendance.

9. Ensemble selon la revendication 8, caractérisé en ce que ledit dispositif (1)comprend en outre :

γ) des moyens de déclenchement, sous l'effet de l'entrée de son code d'activation (C_a), d'une temporisation offrant le temps nécessaire à la rupture et au rétablissement du lien de dépendance, et

δ) des moyens de blocage agissant sur le dispositif (1) si ledit lien de dépendance n'a pas été rétabli avant la fin du temps de temporisation.

10. Ensemble selon la revendication 8 ou 9, caractérisé en ce qu'il comprend, en outre :

ε) des moyens de blocage agissant sur le dispositif (1) en cas d'entrées successives d'un nombre prédéterminé

de codes d'activation erronés.

11. Installation, caractérisée en ce qu'elle est formée :

- d'une pluralité de dispositifs constitués chacun d'un terminal (1) de communication ayant un lien de dépendance avec au moins un composant amovible, dit "composant en place (6,6')", chaque terminal (1) et chaque composant en place (6,6') comportant des clés qui leur sont propres, dites, respectivement, "clé de terminal (C_t)" et "clé de composant (C_c, C_c')", et

- d'un équipement externe (2) comprenant un émetteur-récepteur (4) et une base de données (3), adaptée à enregistrer, pour chaque terminal (1), au moins une donnée identifiant l'utilisateur autorisé, et les informations de clé de terminal (C_t) et de clé de composant (C_c, C_c') qui sont communiquées à l'équipement externe (2) par ledit terminal (1).

12. Installation selon la revendication 11, caractérisée en ce qu'elle comporte en outre :

ζ) des moyens d'envoi, en cas de blocage d'un terminal (1), d'un message d'alerte du terminal concerné vers l'émetteur-récepteur (4) de l'équipement externe (2), ou inversement, ou réciproquement, et éventuellement des moyens d'affichage d'un tel message, lesquels moyens d'envoi/affichage sont activés concomitamment avec lesdits moyens de blocage.

13. Installation selon la revendication 11 ou 12, caractérisée en ce qu'elle comprend en outre :

η) des moyens de déblocage d'un terminal (1) bloqué, moyens qui sont susceptibles d'être mis en oeuvre depuis l'équipement externe (2).

14. Installation selon l'une quelconque des revendications 11 à 13 appliquée à la protection de terminaux (1) dans lesquels sont stockées des données, caractérisée en ce qu'elle comprend en outre :

θ) des moyens de transfert de tout ou partie des données stockées dans le terminal (1) concerné vers la base

de données (3) dudit émetteur-récepteur (4) de l'équipement externe en cas de blocage d'un terminal (1) et/ou

ι) des moyens de destruction de tout ou partie des données stockées dans ledit terminal (1) en cas de blocage de celui-ci.

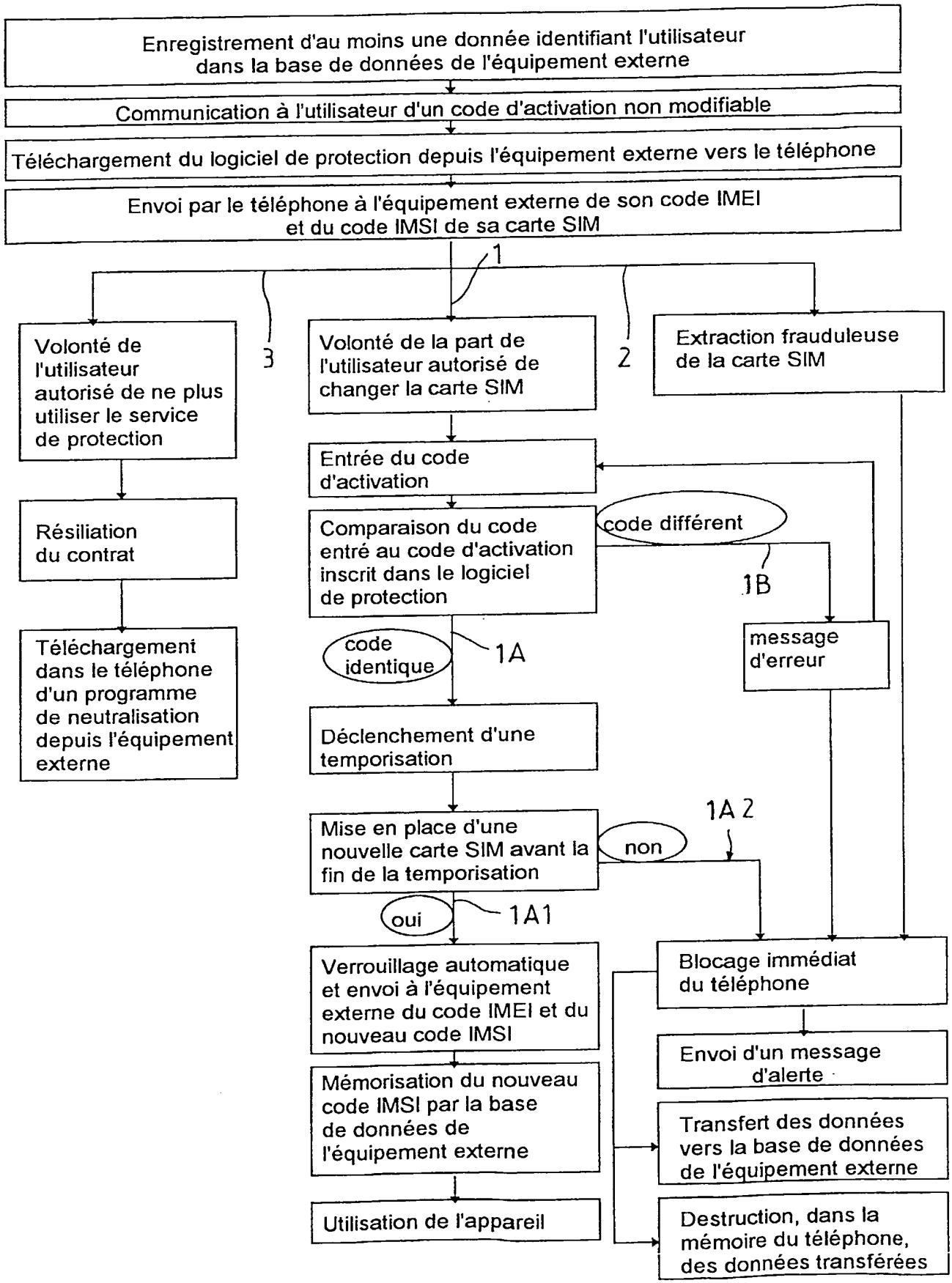

Enregistrement d'au moins une donnée identifiant l'utilisateur dans la base de données de l'équipement externe
Communication à l'utilisateur d'un code d'activation non modifiable
Téléchargement du logiciel de protection depuis l'équipement externe vers le téléphone
Envoi par le téléphone à l'équipement externe de son code IMEI et du code IMSI de sa carte SIM
1
3
2
Volonté de l'utilisateur autorisé de ne plus utiliser le service de protection
Résiliation du contrat
Téléchargement dans le téléphone d'un programme de neutralisation depuis l'équipement externe
Volonté de la part de l'utilisateur autorisé de changer la carte SIM
Extraction frauduleuse de la carte SIM
Entrée du code d'activation
Comparaison du code entré au code d'activation inscrit dans le logiciel de protection
code différent
1B
message d'erreur
code identique
1A
Déclenchement d'une temporisation
Mise en place d'une nouvelle carte SIM avant la fin de la temporisation
non
1A 2
oui
1A1
Verrouillage automatique et envoi à l'équipement externe du code IMEI et du nouveau code IMSI
Mémorisation du nouveau code IMSI par la base de données de l'équipement externe
Utilisation de l'appareil
Blocage immédiat du téléphone
Envoi d'un message d'alerte
Transfert des données vers la base de données de l'équipement externe
Destruction, dans la mémoire du téléphone, des données transférées

Figure 1

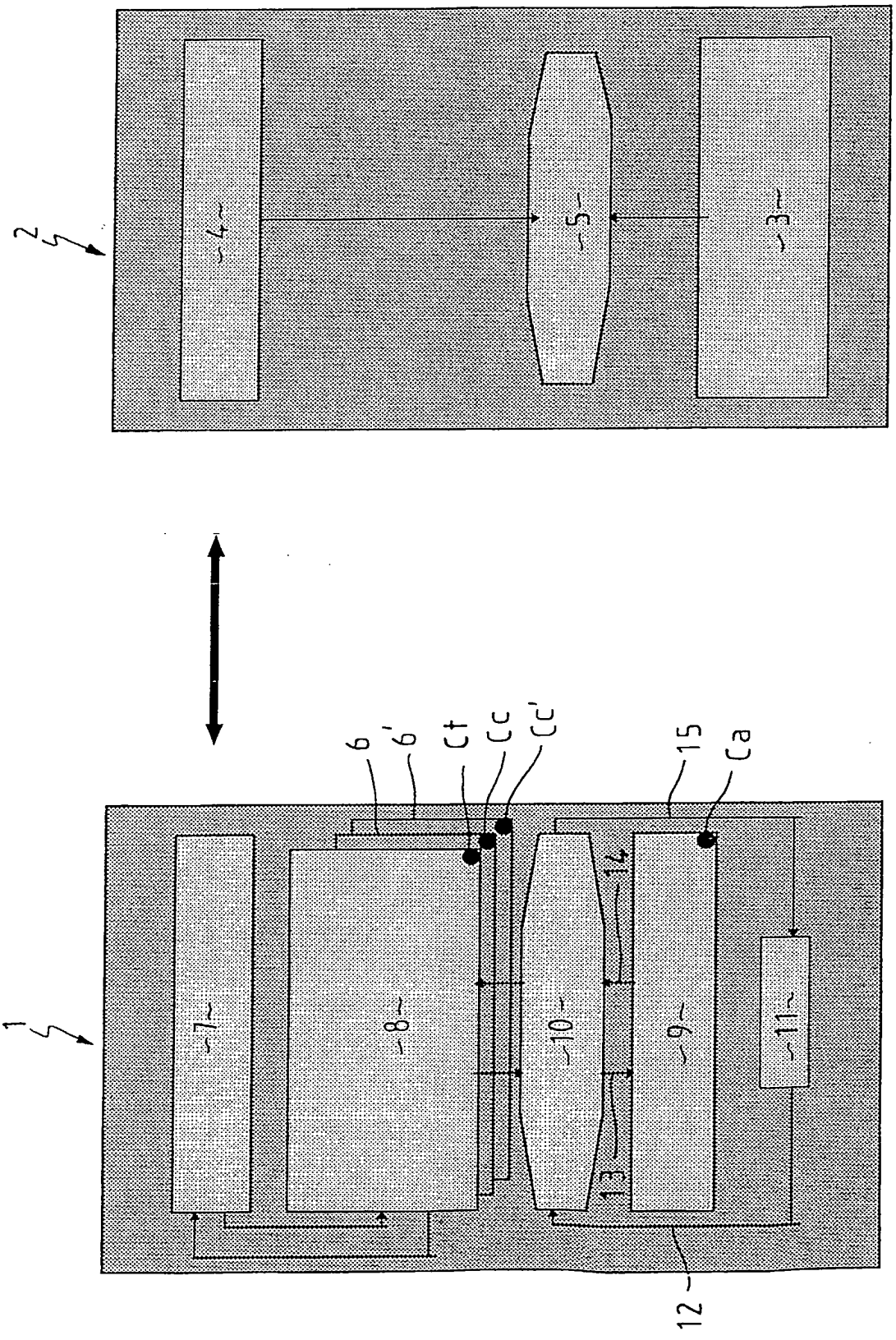


Figure 2

RÉPUBLIQUE FRANÇA

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

2818474

N° d'enregistrement national

FA 599407
FR 0016486

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'Invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	EP 0 776 141 A (NOKIA TELECOMMUNICATIONS OY) 28 mai 1997 (1997-05-28) * colonne 7, ligne 23 - colonne 12, ligne 37 * ---	1-14	H04L9/32 G07F7/10 H04M1/66 G06F17/30 H04Q7/32
A	FR 2 791 509 A (MERMET JEAN PIERRE) 29 septembre 2000 (2000-09-29) * le document en entier * ---	1-14	
A	SCHULTZ C P: "COMMUNICATION DEVICE INACTIVITY PASSWORD LOCK" MOTOROLA TECHNICAL DEVELOPMENTS,US,MOTOROLA INC. SCHAUMBURG, ILLINOIS, vol. 29, 1 novembre 1996 (1996-11-01), pages 91-92, XP000691885 * page 91 * ---	1-14	
A	US 5 996 028 A (OIKAWA TAKEYA ET AL) 30 novembre 1999 (1999-11-30) * colonne 7, ligne 37 - colonne 11, ligne 49 * ---	1-14	
A	US 6 141 563 A (TOOKER JAMES MORRIS ET AL) 31 octobre 2000 (2000-10-31) * colonne 3, ligne 51 - colonne 6, ligne 4 * * revendications * ---	1-14	
A	WO 96 35304 A (NOKIA TELECOMMUNICATIONS OY ;AHVENAINEN JOUKO (FI)) 7 novembre 1996 (1996-11-07) * revendications * -----	1-14	

DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)

H04M
H04Q

Date d'achèvement de la recherche	Examinateur
31 juillet 2001	Roberti, V

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)